HELP ?

James Bond and George Smiley go into business--teaching about business espionage

Journal of Education for Business; Washington; Mar/Apr 1997; Ernest M Teagarden;

Volume: 72
Issue: 4
Start Page: 250-252
ISSN: 08832323
Subject Terms: Industrial espionage

Abstract:
In real life, a solid intelligence organization with realistic goals and adequate financial resources are the real keys to espionage success.

Full Text:

[Headnote]
ABSTRACT. Ask an astute and reasonably well read American about spies and spying, and he or she will think of John LeCarre with his George Smiley, Ian Flemming with his James Bond, or, possibly, Len Deighton and his current hero, Bernard Samson. In real life, a solid intelligence organization with realistic goals and adequate financial resources are the real keys to espionage success.

he end of the Cold War has focused attention on the future role of the U.S. intelligence community. To many, the Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), and other such organizations seem to be underemployed, and new functions must be found to fully use their talents. In addition to monitoring the new Russia and the other post-USSR creations, increased efforts to combat terrorism and drug traffic have been recommended. Support for U.S. commerce and industry in their battle with foreign competition has also been suggested. But how (and if) the nation will use these organizations in economic warfare is far from settled. In the past, intelligence agencies have controlled the export of strategic technology, and the Federal Bureau of Investigation (FBI) has a solid record in combating foreign economic espionage in this country. It has been proposed that the CIA offer direct support to U.S. businesses involved in the export market-a market where competition is increasing at a pace not seen before in American economic history (Fort, 1993).

It is uncertain how well members of the U.S. business community understand the issues involved in international economic warfare. They know the value of computer security, but not many college undergraduates receive instruction in recognizing either domestic or foreign economic espionage activities or in preventing their occurrence. A survey of current business syllabuses and textbooks used in such courses as principles of management, organizational behavior, human resources, or management of technology revealed little or no material on this increasingly important subject. These courses are found in the business curriculum core requirement and are taken by nearly all undergraduate business majors. Graduates are uninformed about business espionage practices despite the fact that such practices have been going on for several hundred years. The FBI and several other government organizations are now trying to correct this deficiency.'

Business intelligence and business espionage are not the same thing, although espionage is usually included under the intelligence label. Business intelligence includes the examination of publicly available information such as court records, corporate annual reports, government documents, market reports, trade fairs, speeches by corporate executives, and reports by sales people. Examination of this material is both legal and ethical. Business espionage is another matter. Espionage exercises are unethical, mostly illegal, and frequently quite innovative: bribing competitors for secret technical processes; hiring

away employees for the sole purpose of obtaining competitors' product, process, or marketing knowledge; doing surreptitious photography; bugging communications (very popular); planting an agent on a competitor's payroll; blackmailing a key employee; or engaging prostitutes to obtain needed information. The list could go on and on.2

Business espionage is not a new phenomenon. In the 18th century, European entrepreneurs stole knowledge of Chinese porcelain processes. The French constructed a factory at Sevres in 1756 only to have its secrets filched by British thieves; these secrets enabled England to dominate the porcelain market almost to the present day. Alfred Krupp stole secrets on steel production processes from the British. Competitors pirated the essentials of Rudolph Diesel's automobile engine before his mysterious disappearance from a British channel steamer in 1914 (Ellis & Nehemkir, 1984).

Industrial espionage is undertaken by U.S. as well as foreign firms; materials and goals vary. Chesebrough-Ponds (CP) was convicted of stealing a breathexercise invention by Harold Hanson. C-P acquired the exerciser specifications during a licensing negotiation with Hanson and then designed a similar device (Ellis & Nehemkir, 1984). Eugene Mayfield, a Proctor and Gamble employee, was caught trying to sell a marketing scheme for Crest toothpaste to Colgate Palmolive for $20,000 (Ellis & Nehemkir). A most interesting story is that of Professor Robert S. Aries of Brooklyn Polytechnic Institute, who used his graduate students as industrial spies. He encouraged his intern-students to bring in their client/employers' trade secrets, which were then sold to competitors. Merck Chemical Company and Sprague Electric Company were both victimized by Aries, who fled to Europe to avoid prosecution and, unless deceased, lives in retirement in France (Ellis & Nehemkir). Other examples are on record in which some of the techniques mentioned earlier in the article were used.

Writing in Who's Stealing Your Business, William Johnson and Jack Maguire (1988) discussed likely espionage objectives. They suggested, among others, product and process information, marketing plans, personnel data, information useful in product counterfeiting, and security techniques. They also argued that it is not only executive and technical experts who may steal. In the same category, they placed administrative assistants, janitors, trash collectors, and equipment installers. Installers who are not in-house should have their credentials carefully examined before admittance to sensitive areas.

Activities by foreign intelligence services in the United States and elsewhere have increased in recent years. The American Society of Industrial Security's 1992 report surveyed 246 U.S. corporations on possible espionage incidents. According to this report, 30% of all detections in 1991 and 1992 had some foreign involvement, up from 21% in the 1985-1988 period. Losses from economic espionage of the 32 largest companies reporting totaled $ 1.8 billion. Pricing data, followed by customer names and product development material, topped the list of information desired. Of the people involved, 58% were either current or former employees. Common methods of obtaining information included break-ins, theft, unauthorized reproduction of data, bribery, and electronic surveillance (Periscope, 1993).3

FBI investigates illegal foreign commercial activities in this country. Most major countries have directed commercial operations against U.S. firms. According to a CIA report issued in 1987, 80% of Japanese intelligence assets are directed against the U.S. and Western Europe (Schweizer, 1993). In Japan, as is commonly known, the link between business and government is stronger than in any other nation. The Ministry of International Trade and Industry (MITI) is the principal link. The Federation of Economic Organizations is another link, which formulates policy recommendations for the Japanese government and acts as a collection vehicle for information (Deacon, 1983). As an example of Japanese economic penetration, Harold Farrar, plant manager for Celanese Corporation in Green, South Carolina, received a payment of $130,000 from Mitsubishi Corporation for data on special celanese film used in x-rays,

overhead observation satellites, and computers (Schweizer, 1993). Fuji Corporation duped Eastman Kodak for years by secretly obtaining technology on its low-priced single-use cameras (Schweizer).

Since 1960, the German intelligence service, Bundesnachrichen (BND), has assigned personnel to spy on research facilities in the United States, Japan, and Italy. In 1989, the BND established Project RAHAB, a computer tracking unit designed to operate against companies in the United States, Japan and Western Europe. (Schweizer). An interesting German technique was used in 1989 when a German visitor to the Du Pont chemical works in Delaware "accidentally" dropped the end of his necktie in a vat of chemicals. Over his protests about the sentimental value of the necktie, Du Pont officials required that the visitor surrender the necktie to the company (Schweizer). The Russians have used similar methods. In 1986, Soviet businessmen visiting the Boeing Aircraft plant in Seattle wore crepe-soled shoes to pick up metal shavings and debris for later analysis. Briefcases with sticky bottoms have been found on other occasions (Johnson & Maguire, 1988).

French agents from the Directorate General de la Securite Exterieure (DGSE) have targeted U.S. corporations for espionage activities since the presidency of Charles de Gaulle (Schweizer, 1993) Some of their efforts have been elaborate and quite costly. In 1980, the DGSE,4 together with the French customs police, tried to blackmail a Swiss banker in an effort to obtain financial information on some of his clients. They planted a stolen Alfa Romeo automobile at a house owned by the banker, M. Stroehin, in the French village of Saillerand-les-Bordes. The banker argued his innocence with the French police and suggested that the desired information could be purchased in Switzerland from one Herr Ralf. The French acted on this suggestion with the result that two French agents were arrested in Switzerland at the time of purchase. Herr Ralf was, in fact, Ralf Elsner, a Swiss security officer (Schweizer). In April 1988, A DGSE team traveled to the Seattle area to monitor tests on a new Boeing 747400 aircraft. The team wanted information on the aircraft's new electronic navigation system, which would eliminate the need for a flight engineer. The team appears to have been successful. Two years later, a similar system was incorporated on the AIRBUS 340, a consortium-produced aircraft involving French participation (Schweizer).

Some professional organizations estimate that only 10% of espionage incidents are actually discovered. America's answer to economic espionage is the FBI, the U.S. Customs Department, and designated units of the U.S. Department of Commerce. All have made their presence known in recent years.

Since 1990, the Department of Justice has prosecuted nearly 50 cases involving economic espionage, the Customs Department has had 400 convictions for similar crimes, and the Department of Commerce has recovered some $4.5 billion in purloined computer software (Michal, 1994). The FBI has warned the U.S. business community about hostile espionage incursions through its Developing Espionage and Counter Intelligence Awareness (DECA) program. The FBI uses other counterintelligence programs and formats (Michal) and maintains a classified list of countries that pose a serious threat to American economic security (Watson, 1992).

The FBI and other governmental units offer personnel and equipment to counter the foreign threat, but some people feel that the CIA should be used as an offensive asset to support the penetration of foreign markets by U.S. business. In a pamphlet, Randall Fort (1993) discussed solid arguments against using the CIA for this purpose. Fort contended that corporate bodies are becoming more complex in structure and their operational areas are becoming wider. Some corporations under U.S. charters conduct the majority of their business in overseas markets, and a number of U.S. corporations are domestically chartered subsidiaries of foreign parents. U.S. firms sometimes participate in joint ventures with foreign partners (Reich, 1990, 1991).5 Which firms should be supported? How much support should be

allowed to each petitioner? What type of support should be given? These questions will not be easy to answer. There also seems to be no great clamor by U.S. executives for CIA assistance. The CIA's experience in **economic intelligence** is largely limited to a few partially effective destabilization programs in Latin America. Such experience does not particularly relate to providing support for U.S. business in foreign markets (Johnson, 1989; Woodward, 1987). William Warner, a lawyer, professor at the University of Kentucky, and former naval intelligence officer, writing in Periscope, suggested several outlets for increased intelligence support. These include counterintelligence, security education, detection of commercial moles,6 and exposure of foreign economic espionage activities, whether under private or government sponsorship (Warner, 1993). His program would have merit for many persons in the intelligence community.

I hope that the above discussion has given some insight into the role that intelligence operations play in both domestic and international trade. With the end of the Cold War, the CIA may be used to help develop a better market for U.S. products overseas-or it may not. Opposition to terrorism and the drug traffic will make demands on CIA resources. The CIA is not experienced in the complexities of world trade. U.S. intelligence forces seem destined to continue education and counterintelligence programs.

U.S. business schools are not teaching the evils of business espionage to their students; syllabuses and textbooks do not include its essentials. Political science students do have curricula dealing with intelligence (including espionage), and most beginning courses have syllabuses and textbooks that contain some information about the activities of the intelligence community. If our business graduates are to understand economic espionage and how to combat it successfully, both faculty and administrators need to recognize its importance.

[Footnote]

NOTES 1. once applied for a small grant from Dakota State University in order to investigate how informative material on economic espionage could be incorporated in a business curriculum. It was rejected by a cross-campus faculty committee. Nevertheless, this university is one institution in which education in the prevention of business espionage was included in organizational behavior courses. 2. A good discussion of the areas and techniques of business espionage may be found in Richard Ellis and Peter Nehemkir (1984). 3. Periscope is a publication of the Association of Former Intelligence Officers. 4. The DGSE was then known as the SDECE or Service de Documentation Exterieure et de Counter-Espionage. In April 1982 the SDECE was changed to the DGSE. The reference to counter-espionage was eliminated in deference to the DST or Direction de la Surveillance du Territoire, the French counterintelligence organization. See Deacon (1990). 5. Robert Reich (1990, 1991) makes the point that the nationality of a corporation depends upon the location of its work force. 6. A mole is an individual who, employed by a firm, secretly provides the firm's restricted information to an outside source(s). In the political sphere, Aldrich Ames and Kim Philby would be considered moles by their respective employers, the CIA and the Secret Intelligence Service (or M16) of Britain.

[Reference]

REFERENCES Deacon, R. (1983). Kemper Tai (pp. 254263). New York: Beaufort Books. Deacon, R. (1990). The French secret service (p. 266). London: Grafton Books. Ellis, R., & Nehemkir, P. (1984). Corporate intelligence and espionage. New York: Macmillan. Fort, R. M. (1993). Economic espionage: Problems and prospects (p. 2). Washington, DC: Consortium for the Study of Intelligence. Johnson, L. K. (1989). America's secret power: The CIA in a democratic society. New York: Oxford University Press. Johnson, W., & Maguire, J. (1988). Who's stealing your business? New York: American Management Association Companies (AMACOM). Michal, K. (1994). Business counter intelligence and the role of the U.S. intelligence community. International Journal of Intelligence and Counter Intelligence, 7(4), 420. Periscope. (1993). IS(5), 3. Reich, R. (1990). Who is us? Harvard Business Review, 68(1), 53-64. Reich, R. (1991). Who is them? Harvard Business Review, 69(2), 77-88. Schweizer, P. (1993). Friendly spies. New York: Atlantic Monthly Press. Warner, W. T. (1993). Economic espionage: A bad idea. Periscope, 18(5), 1. Watson, P. (1992). The FBI's changing missions in the 1990's (pp. 4, 7). Washington, DC: Consortium for the Study of Intelligence. Woodward, R. (1987). Veil: The secret wars of the CIA, 1981-1987. New York: Simon and Schuster.

[Author note]

ERNEST M. TEAGARDEN Dakota State University Madison, South Dakota